ABSTRACT:

A method for securing transmission of streaming media by encrypting each packet in the stream with a packet key using a fast encryption algorithm. The packet key is a hash of the packet tag value and a closed key which is unique for each stream. The closed key is itself encrypted by the sender and passed to the recipient using a public key encryption system. The encrypted closed key (open key) may conveniently be inserted into the stream header. All of the packets in the stream are encrypted, but only the data pay load of each packet is encrypted.

It is computationally infeasible, without knowing the recipient's private key to calculate the closed key based upon knowledge of publicly accessible information such as the recipient's public key, the open key, the encrypted stream data or the packet tag values.